Submitted on: 10.08.2016

Rights to privacy and freedom of expression in public libraries: squaring the circle

David McMenemy
Computer and Information Sciences, University of Strathclyde, Glasgow, United Kingdom.
d.mcmenemy@strath.ac.uk

Abstract:

This paper highlights some of the tensions faced in public libraries in the United Kingdom between the desires to support patrons' rights to privacy and freedom of expressions, versus the reality of modern practice.

Considering both privacy and freedom of expression as ethical concepts, it then discusses some examples from the UK where the tensions between privacy and freedom of expression manifest in practice, including around filtering and government initiatives to tackle extremism, as well as issues around cloud storage of user data. It concludes with a discussion on how public libraries and the profession in the UK must struggle to balance the competing interests of patrons and the state, and encourages the profession to address the tensions head on by regular and rigorous debate as to the issues.

Keywords: privacy, ethics, freedom of expression, public libraries

There are inherent inbuilt tensions between privacy and freedom of expression which pose real challenges for the library and information profession. On one hand, respect for patron privacy allows the patron to seek out information and knowledge that can help them find their place in the world. It is a form of freedom that is cherished by much of the world. Nevertheless, information that one person may deem appropriate to seek out may be deemed by others, rightly or wrongly, as inappropriate or dangerous. This is the heart of the tension between those who advocate respecting privacy and freedom of expression and those who seek to curtail it.

This paper will discuss these tensions and highlight some real scenarios from public libraries in the United Kingdom that reveal the nature of the debate in practice.

The importance of privacy and freedom of expression

Privacy is the "right to be free from unwarranted intrusion and to keep certain matters from public view" (Law, 2015). As such, privacy is an important element in the autonomy of the individual. Much of what makes us human comes from out interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say,

do, and perhaps even feel. If we are not able to trust that we are in a private space, then we may not be completely autonomous, we may hold back crucial elements of ourselves. As Griffin has observed: "frank communication… needs the shield of privacy; it needs the restraint of peeping Toms and eavesdroppers, of phone taps and bugging devices in one's house, of tampering with one's mail or seizure of one's correspondence" (Griffin, 2008, p.225). Without a right to privacy, then, we are not able to be fully ourselves.

Equally, freedom of expression is also about autonomy and self-development. As has been argued, "restrictions on what we are allowed to say and write, or…to hear and read, inhibit our personality and its growth" (Barendt, 2006, p.13). Achieving our potential as human beings is fundamentally about being able to seek out our own path, through access to knowledge that informs our world view and way forward. Under this justification we can also see links between some other fundamental human rights such as the "rights to freedom of religion, thought and conscience" (Barendt, 2006, p.13).

Yet undoubtedly privacy can pose significant challenges to security. If an individual is seeking to commit a crime or a terrorist act, then arguably privacy affords him more opportunity to do so. This is the heart of the tension between a right to privacy and protecting the legitimate interests of others, and the state.

What is important for us to understand in this context is that privacy is a right *qualified* by other interests (as is freedom of expression). What we mean by this is that other rights may take priority over both. This is a perfectly rational notion, since unrestricted privacy or freedom of expression could entail individuals undertaking activities that potentially damage the interests of others or society in general. It does, however, reveal that there is a tension between what a person might expect in terms of privacy (and freedom of expression), and what may be deemed to be encroaching on the rights of others in doing so. Whether we recognise it or not, the intricacies of this qualification lie at the heart of the controversies we face in our professional practice.

In modern times, privacy has been defined as a right that we all should be able to expect to be defended. For instance, Article 12 of the *UDHR* states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The European Convention on Human Rights (ECHR) states both the right to privacy, and the limits that can be placed on it. Article 8 states that: "*Everyone has the right to respect for private and family life, his home and his correspondence."* Section 8 (2) of the ECHR covers the limits that are allowed to be placed on the right to privacy specified in 8(1): *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

In reality, what does this mean? Firstly, that any restrictions placed on the right to privacy by states must be *lawful*. There must be a legal basis for the intrusion, and it must be justified by existing legislation. Framed as they are we can see here a set of restrictions that advocate

invasions of privacy only in terms designed to protect what are deemed to be the legitimate interests of others, whether in the body politic or in their own right.

For librarianship, then, the *qualification* of privacy and what it constitutes in our delivering services to patrons is a vital ethical area that we must seek to have sufficient debating space in as a profession. Much of what our patrons do as a result of using our services is about their self-development and autonomy, and our role in helping them achieve their potential is one we should be justly proud of. Nevertheless, in providing a free and open access to information we must be aware that we are open to critique from those who wish to restrict access for what they deem to be legitimate grounds. We need to have robustly debated all aspects of the arguments for and against if we are to have an influence in how society shapes these fundamental rights.

Our professional values

It is important to acknowledge how much importance we place on privacy and freedom of expression as a profession. As this is a UK-focused paper we will highlight how CILIP advocates for both from the point of view of its ethical principles, however, we will also touch on some of the literature on library values to reinforce the issues.

CILIP states clearly in its statement on intellectual freedom that "Access [to information] should not be restricted on any grounds except that of the law" (CILIP, 2005). On the same pages, CILIP also supports the Council of Europe's approach to accessing information through networked access points from 2000. This reinforces that services providing "Public Access Points should respect the privacy of users and treat knowledge of what they have accessed or wish to access as confidential." Importantly also for our discussion the Council of Europe also state:

> The use by managers of Public Access Points of software filtering systems to block access to certain content is an unwarranted interference with the individual's freedom of access to information. If filtering and blocking systems are to be made available, it should only be as an option that individuals can choose and calibrate at their own preferred levels (CILIP, 2005).

There are however arguments that we must be more pragmatic in our services to patrons, being aware when information may be potentially dangerous for society. Hauptman's landmark experiment in the 1970s where he asked a series of public and academic librarians in the USA for information on how to build a device capable of blowing up a house raised issues of accountability for the profession, in that all libraries asked provided him with the information. While adhering to our core principles, is such a response socially responsible? Hauptman himself later wrote that "censorship must never be confused with the refusal to provide socially detrimental information (in reference), the aiding and abetting of illegal acts, or the judicious selection of materials" (Hauptman, 1988, p.65). One could, of course, argue that personal autonomy of the patron brings with it the responsibility on their part to not do anything with legitimate information that is illegitimate, however, it could equally be argued that professions have a responsibility to not place others in harm's way.

In refusing access to information on a face to face basis, however, we run the risk of having to justify our decision to a patron, and explain in great detail why a legitimate piece of information is not available to them. Blocking access via filtering technologies, on the other

hand, removes that potential embarrassment, and ensures that censorship is carried on out of our view, with little to no input on our part. This lack of having to deal with and justify the restriction of access arguably plays some part in explaining why filtering has been adopted with so little debate by librarians.

In practice.

We will now move to some specific scenarios that highlight the issues around privacy and freedom of expression from the point of view of public libraries in the United Kingdom. While the scenarios may not necessarily provide answers to the dilemmas they highlight, they can raise questions in our minds for further debate.

Much of the controversy around privacy and freedom of expression in public libraries relates to internet filtering. As discussed above, this is a controversial activity that is arguably antithetical to the values of professional librarianship. Nevertheless, it is an activity that is widespread in the United Kingdom. A 2016 study found that 98% of public libraries in the UK filtered categories (Payne, 1016). How such filtering is undertaken raises significant issues for professional practice. The MAIPLE project found that an important dilemma related to the emergence of filtering software was the emergence of filtering software vendors as arbiters of appropriate and inappropriate information types, due to the purchase of off-the-shelf filtering systems with pre-defined categories:

> When it comes to material deemed "inappropriate" rather than unlawful, this can be a very subjective judgement. For formally published material, professional publishers have acted as arbiters of quality or taste and librarians have decided what to include in library collections. When it comes to the internet, it appears that filtering software vendors have a prominent role (Muir et al, 2016).

Two further examples of these issues from research undertaken in our own department are presented below:

- In a 2015 paper, some colleagues and I examined internet acceptable use policies provided by Scottish public libraries from the point of view of language around control and surveillance. In doing so we identified some very loose phraseology with regards to what patrons were requested *not* to access in terms of information types. This included material that was: "grossly offensive" (LA2); "indecent" (LA2, 7, 10, 20, 27 and 28); "disturbing" (LA5, 11, 13, 24 and 26); "depraved" (LA9); "offensive, indecent or menacing" (LA10); "any way that offends decency" (LA3) and "offensive, immoral or distressing" (LA11) (Gallagher, McMenemy and Poulter, 2015).
- In a 2013 paper examining the implementation of filtering in Scottish public libraries (Brown and McMenemy, 2013), it was found that 31 out of 32 public library services in Scotland had installed filtering. Only one stated that frontline staff had the ability to immediately release content blocked by the filter if requested by the user if deemed appropriate, at the point of use: 27 services stated that although there was a "release procedure" in place, the content could not be released at the point of use. It would rather be considered "appropriate" retroactively and released at a later date: two services stated that no procedure existed whereby content blocked by the public access internet filtering software could be released.

This ability or not to unblock filtered content raises important issues around privacy and freedom of expression. In a library context, an argument posited is that all a patron needs do is ask the librarian to unblock any legitimate material that is being withheld by the filtering software, but this is a naïve argument. Consider how many patrons may be too embarrassed to ask a librarian about issues like sexuality; indeed, this may be the primary reason why they have chosen the Internet as their information source as it offers relative anonymity and privacy. Being confronted with a screen blocking access to information is unlikely to have such a patron politely chatting to the person in charge to have their information provided, regardless of their approachability. It could be accurately argued that many organizations ventured down the filtering route to protect the organization rather than in a bid to halt intellectual freedom, but this makes the decision even more problematic for an ethical professional.

While it is certainly true that, as Hauptman puts it, "unfiltered access to the Internet presents some major ethical challenges even to those whose commitment to intellectual freedom is unequivocal," it is equally true that, "it is not our business to mediate between users and the virtual world" (Hauptman, 2002, p.65). As Sturges states, "when people describe internet content as harmful they tend to lump together both legal and illegal material" (Sturges, 2002, p. 21). Whether we can agree or not that some material should be filtered, filters block material that should *not* be filtered. We do our patrons and our profession a disservice by not doing everything we can to clarify this dilemma in our practice.

The Prevent strategy

We have already seen how filtering is cited by libraries in the UK themselves as being useful in blocking "offensive" and "inappropriate" materials. The concern with materials that offend sensibilities, or indeed are perceived as dangerous, is at the heart of the *Prevent* strategy, an initiative of the UK government post 9/11 and renewed after 2011 to tackle "home-grown" terrorism. The strategy's goal is "to prevent radicalisation and stop would-be terrorists from committing mass murder" (HM Government, 2011, p.1) and as such, it focuses on limiting access to and challenging material that has the potential to "radicalize" individuals and inspire them to commit terrorist acts.

The government is at pains to clarify its adherence to the concept of freedom of expression: "We remain absolutely committed to protecting freedom of speech in this country. But preventing terrorism will mean challenging extremist (and non-violent) ideas that are also part of a terrorist ideology" (HM Government, 2011, p.13). However, much of the information it is seeking to limit access to could be classed as reasonable in a democratic country that values freedom of expression, which raises ethical issues for a profession challenged with providing access to legitimate information.

While it is true that *Prevent* has been more controversial in a schools setting than public libraries, there is perhaps an important reason why. A key criterion of *Prevent* is that public bodies providing internet access limit access to information deemed to be potentially harmful:

> we expect local authorities to ensure that publicly- owned venues and resources do not provide a platform for extremists and are not used to disseminate extremist views. This includes considering whether IT equipment available to the general public should use filtering solutions that limit access to terrorist and extremist material (HM Government, 2015)

Therefore, arguably public libraries in the UK were already doing the work of limiting access to such content, rightly or wrongly. It may well be one less thing for them to worry about in

terms of accountability, however, the strategy also acknowledges that "we are unable to determine the extent to which effective filtering is in place in schools and public libraries" (HM Government, 2011, p.79). While a briefing note on *Prevent* from CILIP in 2012 suggested "that libraries have not been subject to interference or intervention" as a result of the strategy, it may well remain a concern for public libraries who buy an off-the-shelf filtering system and install it in the hope that it is the panacea for inappropriate content. CILIP have requested that libraries inform them of any issues with regards the programme.

It is important to note that public libraries in the UK have already been the subject of controversy with regards to access to "extremist" material after the 2007 report, *Hate on the State*, published by a right-leaning think-tank, found that books were found in several libraries that:

- Glorify acts of terrorism against followers of other religions
- Incite violence against anyone who rejects jihadist ideologies
- Endorse violence and discrimination against women (Brandon & Murray, 2007, p.3).

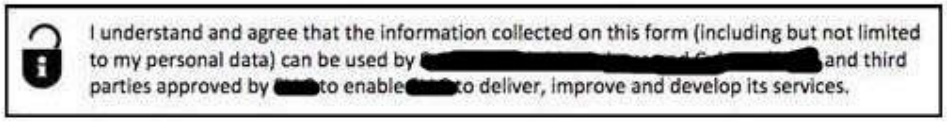
The report gained significant publicity at the time and resulted in the government advisory body developing an advice document on dealing with controversial materials in libraries (Museums, Libraries and Archives Council, 2008).

The emergence of the cloud

One last issue we need to be aware regarding patron privacy relates to a development that on the face of it is progressive rather than regressive. It has largely crept up on us due to the advancement in technology, however, it is one that raises significant issues for privacy, not only for the short term in how we handle the transition, but also significant potential dangers for the long term. This is a form of challenge of the type identified by Michael Gorman: "One of the most obvious prices we are all paying is the actual and potential erosion of privacy caused by the compilation of, and easy access to, large and complex databases resulting from out interaction with commercial, governmental, and other institutions" (Gorman, 2015, p.178).

The ongoing development of software as service (SaS) provides opportunities for library services to work more closely with LMS suppliers, allowing the data from the LMS to be stored in the cloud by the provider themselves rather than by the library service. This clearly has many potential advantages, such as efficiency, and reliability of data access, as well as savings on the costs around staffing to support the processes involved. However, in the UK context, and presumably also in EU areas, this poses challenges for data protection. Under UK law, the data protection statement a member agrees to when they join a library service has to state clearly who is storing the data and for which purposes. Thus, when a library service moves their data to the cloud via a third party, they have to then ask members to agree to a new data protection statement that shows the member has understood and agreed to this. An example of an actual statement emailed to library members of a local authority in Scotland is shown below:

[redacted] Data Protection Statement from July 2015;



To have your details removed from our database please reply to:
unsubscribelibrary@[redacted]

Now such a statement potentially poses significant potential ethical issues. Firstly, not agreeing to the statement means that a membership is no longer valid. In other words, unless the member is happy to agree to the new statement, they can no longer be a library member. Bearing in mind that the public library service in the United Kingdom is *statutory*, this is potentially unfair to the patron.

Secondly, the statement is essentially offering a blanket third party exemption for whom the data can be shared with. Notwithstanding the reassurance that it will only be with third parties the library service *approves*, this is asking the patron to place an element of trust in the service that is ripe for potential future abuse. Not knowing who your data will be shared with, under what pretence, and when, is no recipe for trust. Given that the data concerned involves significant personal information as well as borrowing habits, there is a sense here that convenience and innovation have once again overtaken our duty to debate fully the ramifications of a significant change. What rights does a patron have to challenge an approved provider? What exactly does "enable, deliver, improve, and develop" mean in terms of how data can be used, and the types of organization your data will be passed to? In 10 years' time, as data mining becomes embedded in so much of our lives, will it be prudent for a library service to *approve* selling a third party your data to raise income to buy books? At any point, a member can remove themselves from the database, but doing so means that the right to a library membership ceases, and this seems neither fair nor in the best interests of the patron's autonomy.

In privacy terms, the use of cloud services by libraries to store patron data means we are essentially outsourcing our privacy responsibilities to third parties. This may well be the way of the future, but in doing so we need to be absolutely clear what we are doing, and the potential implications of it down the line. Data protection statements created in haste now can pose significant challenges to patron privacy in years hence.

Conclusions

Public libraries need to tread a line that is deemed to be socially responsible while advocating core values that some in our communities might argue are at best self-indulgent, and at worse potentially dangerous. Only by continuously reinforcing our ethical values in regular debates can we hope to develop the nuanced approach to advocacy that is so crucial in a politically-sensitive time. Our values matter to us, but they serve no other purpose than window dressing if we simply use them to grandstand to members of the community who need reassurance or convincing as to why those values matter.

As *qualified* rights, the adherence of libraries to the rights of both privacy and freedom of expression should not be at the whim of individual librarians, or library committees to

interpret as they please. Equally, we cannot allow our ethical principles to stand as mere monoliths. Our values must be real values, adhered to by our profession wherever possible and always in the forethought of our mind when delivering services to patrons. That our values pose ethical dilemmas for us in practice is a good thing and should be welcomed by us: from debating such dilemmas comes strength of mission.

We have seen evidence in this paper that libraries have introduced practices that arguably challenge our ethical values. The limited debate in the UK profession on such pivotal issues as internet filtering and movement of sensitive data to the cloud challenges our stance as a profession that places privacy and autonomy of patrons at the core of what we do. As a profession, we need to be more upfront about debates around privacy and freedom of expression and continuously be articulating our values in these vital democratic areas. We may fail on occasion, and for legitimate reasons, to hold up to our own ethical standards: but we in no way succeed by pretending we do not have them.

References

Barendt, E. (2005) *Freedom of Speech*. 2nd edition. Oxford: Oxford University Press.

Brandon, J and Murray, D. (2007). *Hate on the State: How British Libraries Encourage Islamic Extremism*, London: Centre for Social Cohesion.

Brown, G.T. and McMenemy, D. (2013), "The implementation of internet filtering in Scottish public libraries", *Aslib Proceedings*, 65 (2), pp.182-202.

CILIP (2005), *CILIP Statement on Intellectual Freedom, Access to Information and Censorship*, London: CILIP. Available from: http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/international/statement-intellectual-freedom-access-information-censorship (accessed 19 July 2016).

CILIP (2012) *The Prevent Strategy: What it means for library and information professionals - A CILIP Briefing paper.* Available from: http://www.cilip.org.uk/sites/default/files/documents/Prevent%20strategy%20briefing%20Jan%202012.pdf (accessed 19 July 2016).

Gallagher, C., McMenemy, D., Poulter, A. (2015) "Management of acceptable use of computing facilities in the public library: avoiding a panoptic gaze?", *Journal of Documentation*, 71(3), pp.572 – 590.

Gorman, M. (2015) *Our enduring values revisited.* Chicago: ALA Publishing.

Griffin, J. (2008) *On Human Rights*. Oxford: Oxford University Press.

Hauptman, R. (1988), *Ethical Challenges in Librarianship*, New York, NY: Oryx Press.

Hauptman, R. (2002) *Ethics and Librarianship.* Jefferson, NC and London: McFarland and Co.

HM Government, (2011) *Prevent strategy*. Command paper 8092. London: Her Majesty's Government.

HM Government, (2015) *Revised* Prevent *Duty Guidance: for Scotland: Guidance for specified Scottish authorities on the duty in the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism.* London: Her Majesty's Government and Edinburgh: The Scottish Government.

Law, J. (2015) *Oxford Dictionary of Law*. Oxford: Oxford University Press.

Muir, A., Spacey, R., Cooke, L., and Creaser , C. (2016) "Regulating internet access in UK public libraries: legal compliance and ethical dilemmas", *Journal of Information, Communication and Ethics in Society*, 14 (1), pp.87 - 104

Museums, Libraries and Archives Council (MLA), 2008. *Guidance on the management of controversial material in public libraries*. London: MLA Council.

Payne, D. (2016) *New research maps the extent of web filtering in public libraries*. Available from: http://www.cilip.org.uk/blog/new-research-maps-extent-web-filtering-public-libraries (accessed 19 July 2016).

Sturges, P. (2002), *Public Internet Access in Libraries and Information Services*. London: Facet.